# Singular integers and $p$-class group of cyclotomic fields

Roland Quême

2009 Oct 19

**Abstract**

Let $p$ be an irregular prime. Let $K = \mathbb{Q}(\zeta)$ be the $p$-cyclotomic field. From Kummer and class field theory, there exist Galois extensions $S/\mathbb{Q}$ of degree $p(p-1)$ such that $S/K$ is a cyclic unramified extension of degree $[S:K] = p$. We give an algebraic construction of the subfields $M$ of $S$ with degree $[M:\mathbb{Q}] = p$ and an explicit formula for the prime decomposition and ramification of the prime number $p$ in the extensions $S/K$, $M/\mathbb{Q}$ and $S/M$. In the last section, we examine the consequences of these results for the Vandiver's conjecture. This article is at elementary level on Classical Algebraic Number Theory.

## Contents



## 1 Some definitions

In this section we give some definitions and notations on cyclotomic fields, $p$-class group, singular numbers, primary and non-primary, used in this paper.

1. Let $p$ be an odd prime. Let $\zeta$ be a root of the polynomial equation $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$. Let $K$ be the $p$-cyclotomic field $K = \mathbb{Q}(\zeta)$ and $O_K$ its ring of integers. Let $K^+$ be the maximal totally real subfield of $K$, $O_{K^+}$ its ring of integers and $O_{K^+}^*$ the group of unit of $O_{K^+}$. Let $v$ be a primitive root $\mod p$ and $\sigma : \zeta \to \zeta^v$ be a $\mathbb{Q}$-automorphism of $K$. Let $G$ be the Galois group of the extension $K/\mathbb{Q}$. Let $\mathbf{F}_p$ be the finite field of cardinal $p$ and $\mathbf{F}_p^*$ its multiplicative group. Let $\lambda = \zeta - 1$. The prime ideal of $K$ lying over $p$ is $\pi = \lambda O_K$.
2. Let $C_p$ be the $p$-class group of $K_p$ (the set of classes whose order is 1 or $p$). Let $r$ be the rank of $C_p$ seen as a $\mathbf{F}_p[G]$-module. If $r > 0$ then $p$ is irregular. Let $C_p^+$ be the $p$-class group of $K_p^+$. Let $r^+$ be the rank of $K_p^+$. Then $C_p = C_p^+ \oplus C_p^-$ where $C_p^-$ is the relative $p$-class group.
3. $C_p$ is the direct sum of $r$ subgroups $\Gamma_i$ of order $p$, each $\Gamma_i$ annihilated by a polynomial $\sigma - \mu_i \in \mathbf{F}_p[G]$ with $\mu_i \in \mathbf{F}_p^*$,

   $$C_p = \oplus_{i=1}^r \Gamma_i. \tag{1}$$

   Then $\mu \equiv v^n \mod p$ with a natural integer $n$, $\quad 1 \leq n \leq p-2$.
4. An integer $A \in O_K$ is said singular if $A^{1/p} \notin K$ and if there exists an ideal $\mathfrak{a}$ of $O_K$ such that $AO_K = \mathfrak{a}^p$. Observe that, with this definition, a unit $\eta \in O_{K^+}^*$ with $\eta^{1/p} \notin O_{K^+}^*$ is singular.
5. A number $A \in K$ is said *semi-primary* if $v_\pi(A) = 0$ and if there exists a natural integer $a$ such that $A \equiv a \mod \pi^2$. A number $A \in K$ is said *primary* if $v_\pi(A) = 0$ and if there exists a natural integer $a$ such that $A \equiv a^p \mod \pi^p$. Clearly a primary number is semi-primary. A number $A \in K$ is said *hyper-primary* if $v_\pi(A) = 0$ and if there exists a natural integer $a$ such that $A \equiv a^p \mod \pi^{p+1}$.

# 2 Some preliminary results

In this section we recall some properties of singular numbers given in Quême [5] in theorems 2.4 p. 4, 2.7 p. 7 and 3.1 p. 9. Let $\Gamma$ be one of the $r$ subgroups $\Gamma_i$ defined in relation (1).

1. $\underline{\text{If } r^- > 0 \text{ and } \Gamma \subset C_p^-:}$ then there exist singular semi-primary integers $A$ with $\underline{AO_K = \mathfrak{a}^p}$ where $\mathfrak{a}$ is a **non**-principal ideal of $O_K$ and verifying simultaneously

   $$\begin{aligned} & Cl(\mathfrak{a}) \in \Gamma,\ Cl(\mathfrak{a}^{\sigma-\mu}) = 1, \\ & \sigma(A) = A^\mu \times \alpha^p, \quad \mu \in \mathbf{F}_p^*, \quad \alpha \in K, \\ & \mu \equiv v^{2m+1} \mod p, \quad m \in \mathbb{N}, \quad 1 \leq m \leq \frac{p-3}{2}, \\ & \pi^{2m+1} \mid A - a^p, \quad a \in \mathbb{N}, \quad 1 \leq a \leq p-1. \end{aligned} \tag{2}$$

In that case we say that $A$ is a *negative* singular integer to point out that $Cl(\mathfrak{a}) \in C_p^-$. Moreover, this number $A$ verifies

$$A \times \overline{A} = D^p, \tag{3}$$

for some integer $D \in O_{K^+}^*$.

(a) Either $A$ is singular non-primary with $\pi^{2m+1} \parallel A - a^p$.

(b) Or $A$ is singular primary with $\pi^p \mid A - a^p$. In that case we know from class field theory that $r^+ > 0$.

(see Quême [5] theorem 2.4 p. 4). The singular primary negative numbers are interesting because they exist if and only if $h^+ \equiv 0 \bmod p$ (the Vandiver conjecture is false).

2. If $r^+ > 0$ and $\Gamma \subset C_p^+$: then there exist singular semi-primary integers $A$ with $AO_K = \mathfrak{a}^p$ where $\mathfrak{a}$ is a **non**-principal ideal of $O_K$ and verifying simultaneously

$$\begin{aligned}
&Cl(\mathfrak{a}) \in \Gamma,\ Cl(\mathfrak{a}^{\sigma-\mu}) = 1,\\
&\sigma(A) = A^\mu \times \alpha^p, \quad \mu \in \mathbf{F}_p^*, \quad \alpha \in K,\\
&\mu \equiv v^{2m} \bmod p, \quad m \in \mathbb{Z}, \quad 1 \le m \le \frac{p-3}{2},\\
&\pi^{2m} \mid A - a^p, \quad a \in \mathbb{Z}, \quad 1 \le a \le p-1,
\end{aligned} \tag{4}$$

In that case we say that $A$ is a *positive* singular integer to point out that $Cl(\mathfrak{a}) \in C_p^+$. Moreover, this integer $A$ verifies

$$\frac{A}{\overline{A}} = D^p, \tag{5}$$

for some number $D \in K_p^+$. If $h^+ \equiv 0 \bmod p$ then $D \neq 1$ is possible, for instance with $\mathfrak{a} = \mathfrak{q}$ where $\mathfrak{q}$ is a prime ideal of $O_K$, $Cl(\mathfrak{q}) \in C_p^+$ and $q \equiv 1 \bmod p$.

(a) Either $A$ is singular non-primary with $\pi^{2m} \parallel A - a^p$ .

(b) Or $A$ is singular primary with $\pi^p \mid A - a^p$.

(see Quême, [5] theorem 2.7 p. 7).

3. If $\mu \equiv v^{2m} \bmod p$ with $1 \le m \le \frac{p-3}{2}$: then there exist singular units $A \in O_{K^+}^*$ with

$$\begin{aligned}
&\sigma(A) = A^\mu \times \alpha^p, \quad \mu \in \mathbf{F}_p^*, \quad \alpha \in O_{K^+}^*,\\
&\mu \equiv v^{2m} \bmod p, \quad m \in \mathbb{Z}, \quad 1 \le m \le \frac{p-3}{2},\\
&\pi^{2m} \mid A - a^p, \quad a \in \mathbb{Z}, \quad 1 \le a \le p-1,
\end{aligned} \tag{6}$$

(a) Either $A$ is non-primary with $\pi^{2m} \parallel A - a^p$ .

(b) Or $A$ is primary with $\pi^p \mid A - a^p$.

(see Quême, [5] theorem 3.1 p. 9).

The sections 3, 4 and 5 are, for a large part, a reformulation of Hilbert theory of *Kummer Fields*, see [1] paragraph 125 p. 225.

# 3 Singular $K$-extensions

**Some Definitions** :

1. In this section, let us denote $\Gamma$ one of the $r$ subgroups of order $p$ of $C_p$ defined by relation (1). Let $A$ be a singular semi-primary integer, negative or positive, verifying respectively the relations (2) or (4) . We call $S = K(A^{1/p})/K$ a singular negative, respectively positive $K$-extension if $\Gamma \in C_p^-$, respectively $\Gamma \in C_p^+$.
2. Let $A$ be a singular unit verifying the relation (6). We call $S = K(A^{1/p})/K$ a singular unit $K$-extension.
3. A singular $K$-extension $S = K(A^{1/p})$ is said primary or non-primary if the singular number $A$ is primary or non-primary.
4. If $S$ is primary then the extension $S/K$ is, from Hilbert class field theory, the cyclic unramified extension of degree $p$ corresponding to $\Gamma$.
5. Observe that the extensions $S/\mathbb{Q}$ are Galois extensions of degree $p(p-1)$.

**Lemma 3.1.** *There is one and only one singular negative $K$-extension corresponding to a group $\Gamma \subset C_p^-$.*

*Proof.* For $\Gamma$ given let us consider two singular negative $K$-extensions $S/K$ and $S'/K$. $AO_K = \mathfrak{a}^p$ and $A'O_K = \mathfrak{a}'^p$. The polynomial $\sigma - \mu$ annihilates $< Cl(\mathfrak{a} >$ and $< Cl(\mathfrak{a}' >$. Then $< Cl(\mathfrak{a}) > = < Cl(\mathfrak{a}') > = \Gamma$, thus there exists $n,\ 1 \leq n \leq p-1$ such that $Cl(\mathfrak{a}^n) = Cl(\mathfrak{a}')$. Therefore $A^n = A' \times \gamma^p \times \varepsilon,\ \varepsilon \in O_K^*,\ \gamma \in K$. It follows, from $A\overline{A} = D^p$ and $A'\overline{A}' = D'^p$ with $D, D' \in O_{K+}$, that $\varepsilon\overline{\varepsilon} \in O_{K+}^{*p}$. Therefore $\varepsilon = \zeta^w \varepsilon_1^p,\ \varepsilon_1 \in O_{K+}^*$. Then $A^n = A'\gamma^p\zeta^w\varepsilon_1^p\zeta^w$. $A$ and $A'$ are semi-primary, thus it follows that $w = 0$. Therefore $K(A^{1/p}) = K(A'^{1/p})$. ∎

**Remark:** Observe that we consider in this article only singular semi-primary numbers. Let $A$ be a singular semi-primary number. Then $A' = A\zeta$ is not semi-primary and $K(A^{1/p}) \neq K(A^{1/p})$.

**Lemma 3.2.** *If $\mu \neq 1$ and $\mu^{(p-1)/2} \equiv 1$ mod $p$ there is one and only one singular unit $K$-extension $S/K$ depending only on $\mu$.*

*Proof.* The subgroup of $O^*_{K^+}/O^{*p}_{K^+}$ annihilated by $\sigma - \mu$ is of order $p$ and the rank of $O^*_{K^+}/O^{*p}_{K^+}$ is $\frac{p-3}{2}$. □

**Lemma 3.3.** *$\pi$ is the only prime which can ramify in the singular $K$-extension $S/K$ and the relative discriminant of $S/K$ is a power of $\pi$.*

*Proof.* $S/K$ is unramified except possibly at $\pi$, (see for instance Washington [8] exercise 9.1 (b) p. 182). The result for relative discriminant follows. □

**Lemma 3.4.**

1. *There are $r^+$ singular primary negative $K$-extensions $S/K$.*
2. *There are $r^- - r^+$ singular non-primary negative $K$-extensions $S/K$.*

*Proof.* The first part results of classical theory of $p$-Hilbert class field applied to the field $K$ and of previous definition of singular $K$-extensions $S_\mu$ (see for instance the result of Furtwangler in Ribenboim [6] (6C) p. 182) and the second part is an immediate consequence of the first part. □

# 4 Singular $\mathbb{Q}$-fields

Let $A$ be a semi-primary integer, negative (see definition (2)), positive (see definition (4)) or unit (see definition (6)). Let $\omega$ be an algebraic number defined by

$$\omega = A^{(p-1)/p}. \tag{7}$$

We had chosen this definition instead of $\omega = A^{1/p}$ because $A^{p-1} \equiv 1 \bmod \pi$ simplifies computations. Then $S = K(\omega)$ is the corresponding singular $K$-extension. Observe that this definition implies that $\omega \in O_S$ ring of integers of $S$.

**Lemma 4.1.** *Suppose that $S/K$ is a singular primary $K$-extension. Let $\theta : \omega \to \omega\zeta$ be a $K$-isomorphism of the field $S$. Then, $A$ is hyperprimary and there are $p$ prime ideals of $O_S$ lying over $\pi$. There exists a prime ideal $\pi_0$ of $O_S$ lying over $\pi$ such that the $p$ prime ideals $\pi_n = \theta^n(\pi_0)$, $n = 0, \dots, p-1$ of $O_S$ lying over $\pi$ verify the congruences*

$$\begin{aligned} &\pi_0^2 \mid \omega - 1, \\ &\pi_n \parallel \omega - 1, \ \dots, n = 1, \dots, p-1. \end{aligned} \tag{8}$$

*Proof.*

1. From Hilbert class field theory and Principal Ideal Theorem the prime principal ideal $\pi$ of $K$ splits totally in the extension $S/K$. The ideal $\pi$ does not correspond to the case III.c in Ribenboim [6] p. 168 because $\pi$ is not ramified in $S/K$. The ideal $\pi$ does not correspond to the case III.b in Ribenboim [6] p. 168 because $\pi$ is not inert in $S/K$. Therefore $\pi$ corresponds to the case III.a and it follows that there exists $a_1 \in O_K$ such that $A \equiv a_1^p \bmod \pi^{p+1}$. Therefore there exists $a \in \mathbb{Z}$ such that $a \equiv a_1 \bmod \pi$ and $A \equiv a^p \bmod \pi^{p+1}$, thus $A$ is a singular hyper-primary number and $A^{p-1} \equiv 1 \bmod \pi^{p+1}$.
2. Then $\omega^p - 1 \equiv 0 \bmod \pi^{p+1}$. Let $\theta : \omega \to \omega\zeta$ be a $K$-automorphism of the field $S$. Let $\Pi'$ is any of the $p$ prime ideals of $O_S$ lying over $\pi$. Then $\pi O_S = \prod_{n'=0}^{p-1} \pi_{n'}$ where $\pi'_n = \theta^n(\Pi'),\ n = 0, \dots, p-1$ are the $p$ prime ideals of $O_S$ lying over $\pi$.
3. From $A^{p-1} \equiv 1 \bmod \pi^{p+1}$ we see that

$$\omega^p - 1 = \prod_{n=0}^{p-1} (\omega\zeta^{-n} - 1) \equiv 0 \bmod \pi_0'^{p+1} \pi_1'^{p+1} \dots \pi_{p-1}'^{p+1}.$$

   It follows that there exists a prime ideal $\Pi$ of $O_S$ lying over $\pi$ such that $\omega - 1 \equiv 0 \bmod \Pi^2$ because there exists $l$ such that $\omega\zeta^l - 1 \equiv 0 \bmod \pi_0'^2)$ so $\Pi = \theta^{-l}(\pi'_0$, and that $\Pi \parallel \omega\zeta^{-n} - 1$ for $n = 1, \dots, p-1$ because $\Pi \parallel \zeta - 1$. Let us note $\pi_n = \theta^n(\Pi)$ for $n = 0, \dots, p-1$. It follows that, for $n = 1, \dots, p-1$, $\pi_n \parallel \omega\zeta^n\zeta^{-n} - 1$ and so

$$\begin{aligned} &\pi_0^2 \mid \omega - 1, \\ &\pi_n \parallel \omega - 1,\ \dots, n = 1, \dots, p-1. \end{aligned} \tag{9}$$

$\square$

**Lemma 4.2.** *Suppose that $S/K$ is a singular non primary $K$-extension. Let $\Pi$ be the prime of $S$ lying over $\pi$. Then $\Pi \mid \omega - 1$.*

*Proof.* The extension $S/K$ is ramified therefore $\pi O_S = \Pi^p$. $A^{p-1} \equiv 1 \bmod \pi^n$ for some $n > 1$ and so $\omega^p - 1 \equiv 1 \bmod \Pi^{np}$ because $\pi O_S = \Pi^p$. Therefore $\omega \equiv 1 \bmod \Pi$. $\square$

We know that there are $p$ different automorphisms of the field $S$ extending the $\mathbb{Q}$-automorphism $\sigma$ of the field $K$.

**Lemma 4.3.** *There exists an automorphism $\sigma_\mu$ of $S/\mathbb{Q}$ extending $\sigma$ such that*

$$\omega^{\sigma_\mu - \mu} \equiv 1 \ mod\ \pi^2. \tag{10}$$

*Proof.*

From $\sigma(A) = A^\mu \alpha^p$ there exist $p$ different automorphisms $\sigma_{(w)},\ w = 0, \dots, p-1$, of the field $S$ extending the $\mathbb{Q}$-isomorphism $\sigma$ of the field $K$, defined by

$$\sigma_{(w)}(\omega) = \omega^\mu \alpha^{p-1} \zeta^w, \tag{11}$$

for natural numbers $w = 0, 1, \dots, p-1$. There exists one and only one $w$ such that $\alpha^{p-1} \times \zeta^w$ is a semi-primary number (or $\alpha^{p-1} \times \zeta^w \equiv 1 \bmod \pi^2$). Let us set $\sigma_\mu = \sigma_{(w)}$ to emphasize the role of $\mu$ Therefore we get

$$\sigma_\mu(\omega) \equiv \omega^\mu \bmod \pi^2, \tag{12}$$

because $\omega, \sigma_\mu(\omega) \in O_S$. □

**Lemma 4.4.** $\sigma_\mu^{p-1}(\omega) = \omega$.

*Proof.* We have $\sigma_\mu^{p-1}(A) = \sigma^{p-1}(A) = A$ therefore there exists a natural integer $w_1$ such that $\sigma_\mu^{p-1}(\omega) = \omega \times \zeta^{w_1}$. We have proved in relation (12) that

$$\sigma_\mu(\omega) \equiv \omega^\mu \bmod \pi^2, \tag{13}$$

thus $\sigma_\mu^{p-1}(\omega) \equiv \omega^{\mu^{p-1}} \equiv \omega \times A^{(p-1)(\mu^{p-1}-1)/p} \equiv \omega \bmod \pi^2$ which implies that $w_1 = 0$ and that $\sigma_\mu^{p-1}(\omega) = \omega$. □

Let us define $\Omega \in O_S$ ring of integers of $S$ by the relation

$$\Omega = \sum_{i=0}^{p-2} \sigma_\mu^i(\omega). \tag{14}$$

**Theorem 4.5.** *$M = \mathbb{Q}(\Omega)$ is a field with $[M : \mathbb{Q}] = p$, $[S : M] = p-1$ and $\sigma_\mu(\Omega) = \Omega$.*

*Proof.*

1. Show that $\Omega \neq 0$: If $S/K$ is unramified, then $\omega \equiv 1 \bmod \pi$ implies with definition of $\Omega$ that $\Omega \equiv p-1 \bmod \pi$ and so $\Omega \neq 0$. If $S/K$ is ramified, then $\omega \equiv 1 \bmod \Pi$ implies with definition of $\Omega$ that $\Omega \equiv p-1 \bmod \Pi$ because $\sigma_\mu(\Pi) = \Pi$ and so $\Omega \neq 0$.
2. Show that $\Omega \notin K$: from $\sigma_\mu(\omega) = \omega^\mu \alpha^{p-1} \zeta^w$ we get

   $$\Omega = \sum_{i=0}^{p-2} \omega^{\mu^i \bmod p} \times \beta_i,$$

   with $\beta_i \in K$. Putting together terms of same degree we get $\Omega = \sum_{j=1}^{p-1} \gamma_j \omega^j$ where $\gamma_j \in K$ are not all null because $\Omega \neq 0$. $\Omega \in K$ should imply the polynomial equation $\sum_{j=1}^{p-1} \omega^j \times \gamma_j - \gamma = 0$ with $\gamma \in K$, not possible because the minimal polynomial equation of $\omega$ with coefficients in $K$ is $\omega^p - A^{p-1} = 0$.

3. Show that $M = \mathbb{Q}(\Omega)$ verifies $M \subset S$ with $[M : \mathbb{Q}] = p$ and $[S : M] = p - 1$: $S/\mathbb{Q}$ is a Galois extension with $[S : \mathbb{Q}] = (p - 1)p$. Let $G_S$ be the Galois group of $S/\mathbb{Q}$. Let $< \sigma_\mu >$ be the subgroup of $G_S$ generated by the automorphism $\sigma_\mu \in G_S$. We have seen in lemma 4.4 that $\sigma_\mu^{p-1}(\omega) = \omega$. In the other hand $\sigma_\mu^{p-1}(\zeta) = \zeta$ and $\sigma_\mu^n(\zeta) \neq \zeta$ for $n < p - 1$ and so $< \sigma_\mu >$ is of order $p - 1$.
4. From fundamental theorem of Galois theory, there is a fixed field $M = S^{<\sigma_\mu>}$ with $[M : \mathbb{Q}] = [G_S :< \sigma_\mu >] = p$. From $\sigma_\mu(\Omega) = \Omega$ seen and from definition relation (14) it follows that $\Omega \in M$ and from $\Omega \notin K$ it follows that $M = \mathbb{Q}(\Omega)$. Thus $S = M(\zeta)$ and $\omega \in S$ can be written

$$\omega = 1 + \sum_{i=0}^{p-2} \omega_i \lambda^i,\ \omega_i \in M. \tag{15}$$

with $\lambda = \zeta - 1$ and with $\sigma_\mu(\omega_i) = \omega_i$ because $\sigma_\mu(\Omega) = \Omega$.

$\square$

**Some definitions:** The field $M \subset S$ is called a singular $\mathbb{Q}$-field. In the sequel of this paper we are studying some algebraic properties and ramification of singular $\mathbb{Q}$-fields $M$. A singular $\mathbb{Q}$-field $M$ is said primary (respectively non-primary) if $S$ is a singular primary (respectively non-primary) $K$-extension.

# 5 Algebraic properties of singular $\mathbb{Q}$-fields

1. From Galois theory there are $p$ subfields $M_i,\ i = 0, \dots, p - 1$, of $S$ of degree $[M_i : \mathbb{Q}] = p$.
2. The extension $S/\mathbb{Q}$ is Galois. Let $\theta : \omega \to \omega\zeta$ be a $K$-automorphism of $S$. There are $p$ automorphisms $\sigma_i,\ i = 0, \dots, p - 1$, of $S$ extending the $\mathbb{Q}$-automorphism $\sigma$ of $K$ verifying $\sigma_i(\theta^i(\omega)) = (\theta^i(\omega))^\mu \beta$ for the semi-primary $\beta \in K$.
3. We have defined in relation (14) $\Omega = \sum_{k=0}^{p-2} \sigma_\mu^k(\omega)$. For $i = 1, \dots, p - 1$ we can define similarly $\Omega_i = \sum_{k=0}^{p-2} \sigma_\mu^k(\theta^i(\omega))$. Then we show in following result that the fields $M_i$ can be explicitly defined by $M_i = \mathbb{Q}(\Omega_i),\ i = 0, \dots, p - 1$.

**Lemma 5.1.** *The singular $\mathbb{Q}$-fields $M_i = \mathbb{Q}(\Omega_i), \dots, p-1$, are the $p$ subfields of degree $p$ of the singular $K$-extension $S/K$.*

*Proof.*

1. We set here $\sigma_0 = \sigma_\mu$ and $M_0 = M$. Show that the fields $M_0, M_1, \dots, M_{p-1}$ are pairwise different: $\sigma_i(\theta^i(\omega)) = (\theta^i(\omega))^\mu \beta$, hence $\sigma_i(\omega\zeta^i) = (\omega\zeta^i)^\mu \beta$, hence

$$\sigma_i(\omega) = \omega^\mu \beta \zeta^{i(\mu - v)}. \tag{16}$$

Suppose that $M_i = M_{i'}$: then the subgroups $< \sigma_i >$ and $< \sigma_{i'} >$ of $Gal(S/\mathbb{Q})$ corresponding to the fixed fields $M_i$ and $M_{i'}$ are equal. Therefore there exists a natural integer $l$, $1 \le l \le p-2$ coprime with $p-1$ such that $\sigma_{i'} = \sigma_i^l$.

2. $\sigma_{i'}(\zeta) = \sigma_i^l(\zeta)$, hence $\zeta^v = \zeta^{v^l}$, hence $v \equiv v^l \mod p$, hence $v^{l-1} \equiv 1 \mod p$, hence $l - 1 \equiv 0 \mod p-1$ and therefore $l \equiv 1 \mod p-1$. In the other hand $1 \le l \le p-2$, thus $l = 1$ and $\sigma_i(\omega) = \sigma_{i'}(\omega)$. From relation (16) this implies that $i = i'$.

□

In the following theorem, we give an explicit computation of $\Omega_i$ for $i = 0, \dots, p-1$. Let us denote $\mu_k$ for $\mu^k \mod p$.

**Lemma 5.2.** *The subfields of degree p of the singular $K$-extension $S$ are the singular $\mathbb{Q}$-fields $M_i = \mathbb{Q}(\Omega_i)$, $i = 0, \dots, p-1$, where*

$$\begin{aligned} \Omega_i = \theta^i(\Omega) &= \sum_{k=0}^{p-2} \omega^{\mu^k} \beta^{(\sigma^k - \mu^k)/(\sigma - \mu)} \zeta^{i\mu^k}, \\ \Omega_i = \theta^i(\Omega) &= \sum_{k=0}^{p-2} \omega^{\mu_k} A^{(p-1)(\mu^k - \mu_k)/p} \beta^{(\sigma^k - \mu^k)/(\sigma - \mu)} \zeta^{i\mu^k}. \end{aligned} \tag{17}$$

*Proof.* We start of $\Omega_i = \sum_{k=0}^{p-2} \sigma_i^k(\theta^i(\omega))$ and we compute $\sigma_i^k(\theta^i(\omega))$. Let us note $\varpi_i = \theta^i(\omega)$. $\sigma_i(\varpi_i) = \varpi_i^\mu \beta$, hence $\sigma_i^2(\varpi_i) = \sigma(\varpi_i)^\mu \sigma(\beta) = (\varpi_i^\mu \beta)^\mu \sigma(\beta) = \varpi_i^{\mu^2} \beta^{\sigma+\mu}$. Pursuing up to $k$, we get $\sigma_i^k(\varpi_i) = \varpi_i^{\mu^k} \beta^{(\sigma^k - \mu^k)/(\sigma-\mu)}$. But $\varpi_i^{\mu^k} = (\omega\zeta^i)^{\mu^k} = \omega^{\mu^k} \zeta^{i\mu^k}$. We can also compute at first $\Omega = \sum_{k=0}^{p-2} \omega^{\mu^k} \beta^{(\sigma^k - \mu^k))/(\sigma-\mu)}$ and then verify directly that $\theta^i(\Omega) = \Omega_i$. Then $\omega^{\mu^k} = \omega^{\mu_k} A^{(p-1)(\mu^k - \mu_k)/p}$. □

# 6 The ramification in the singular primary $\mathbb{Q}$-fields

1. Observe at first that the case of singular non-primary $\mathbb{Q}$-fields can easily be described. The extension $S/K$ is fully ramified at $\pi$, so $pO_S = \pi_S^{p(p-1)}$. Therefore there is only one prime ideal $\mathfrak{p}$ of $M$ ramified with $pO_M = \mathfrak{p}^p$.

2. The end of this section deals with the ramification of singular primary $\mathbb{Q}$-fields $M$. In that case $S/K$ is a cyclic unramified extension and there are $p$ prime ideals in $S/K$ over $\pi$.

**Lemma 6.1.** $\sigma_\mu(\pi_0) = \pi_0$

*Proof.* From relation (13) $\sigma_\mu(\omega) \equiv \omega^\mu \bmod \pi^2$. From lemma 4.1 $\omega \equiv 1 \bmod \pi_0^2$ and so $\sigma_\mu(\omega) \equiv \omega^\mu \equiv 1 \bmod \pi_0^2$. Then $\omega \equiv 1 \bmod \sigma_\mu^{-1}(\pi_0)^2$. If $\sigma_\mu^{-1}(\pi_0) \neq \pi_0$ it follows that $\omega \equiv 1 \bmod \pi_0^2 \times \sigma^{-1}(\pi_0^2)$, which contradicts lemma 4.1. □

**Lemma 6.2.** *Let $\pi_k = \theta^k(\pi_0)$ for any $k \in \mathbb{N}, \quad 1 \leq k \leq p-1$. Then $\sigma_\mu(\pi_k) = \pi_{n_k}$ with $n_k \in \mathbb{N}, \quad n_k \equiv k \times v\mu^{-1}$ mod $p$.*

*Proof.*

1. From $\pi_0^2 \mid (\omega - 1)$, it follows that $\theta^k(\pi_0^2) = \pi_k^2 \mid (\omega\zeta^k - 1)$. Then

$$\sigma_\mu(\pi_k)^2 \mid (\sigma_\mu(\omega) \times \zeta^{vk} - 1).$$

2. We have $\sigma_\mu(\pi_k) = \pi_{k+l_k}$ for some $l_k \in \mathbb{N}$ depending on $k$. From relation (13) we know that $\sigma_\mu(\omega) \equiv \omega^\mu \bmod \pi^2$. Therefore

$$\pi_{k+l_k}^2 \mid (\omega^\mu \times \zeta_p^{vk} - 1).$$

3. In an other part by the $K$-automorphism $\theta^{k+l_k}$ of $S$ we have

$$\pi_{k+l_k}^2 \mid (\omega \times \zeta^{k+l_k} - 1),$$

so

$$\pi_{k+l_k}^2 \mid (\omega^\mu \times \zeta^{\mu(k+l_k)} - 1).$$

4. Therefore $\pi_{k+l_k}^2 \mid \omega^\mu(\zeta^{vk} - \zeta^{\mu(k+l_k)})$, and so

$$\pi_{k+l_k}^2 \mid (\zeta^{vk} - \zeta^{\mu(k+l_k)}),$$

5. This implies that $\mu(k+l_k) - vk \equiv 0 \bmod p$, so $\mu l_k + k(\mu - v) \equiv 0 \bmod p$ and finally that

$$l_k \equiv k \times \frac{v-\mu}{\mu},$$

where we know that $v - \mu \not\equiv 0 \bmod p$ from Stickelberger relation. Then $n_k \equiv k + k \times \frac{v-\mu}{\mu} = k \times \frac{v}{\mu} \bmod p$, which achieves the proof.

□

**Lemma 6.3.**

1. *If $S/K$ is a singular primary negative extension then $\sigma_\mu^{(p-1)/2}(\pi_k) = \pi_k$.*
2. *If $S/K$ is a singular primary positive or unit extension then $\sigma_\mu^{(p-1)/2}(\pi_k) = \pi_{n-k}$.*

*Proof.* From lemma 6.2 we have $\sigma_\mu^{(p-1)/2}(\pi_k) = \pi_{k'}$ with $k' \equiv kv^{(p-1)/2}\mu^{-(p-1)/2}$. If $S/K$ is negative then $v^{(p-1)/2}\mu^{-(p-1)/2} \equiv 1 \bmod p$ and if $S/K$ is positive or unit then $v^{(p-1)/2}\mu^{-(p-1)/2} \equiv -1 \bmod p$ and the result follows. □

**Lemma 6.4.** *The length of the orbit of the action of the group $<\sigma_\mu>$ on $\pi_0$ is 1 and the length of the orbit of the action of the group $<\sigma_\mu>$ on $\pi_i,\ i = 1, \dots, p-1$ is $d$ where $d$ is the order of $v\mu^{-1}$ mod $p$.*

*Proof.* For $\pi_0$ see lemma 6.1. For $\pi_k$ see lemma 6.2: $\sigma_\mu(\pi_k) = \sigma(\pi_{n_k})$ with $n_k \equiv v\mu^{-1} \bmod p$, then $\sigma_\mu^2(\pi_k) = \sigma(\pi_{n_{k_2}})$ with $n_{k_2} \equiv kv^2\mu^{-2} \bmod p$ and finally $n_{k_d} \equiv k \bmod p$. □

The only prime ideals of $M/\mathbb{Q}$ ramified are lying over $p$. The prime ideal of $K$ over p is $\pi$. To avoid cumbersome notations, the prime ideals of $S$ over $\pi$ are noted here $\Pi$ or $\Pi_i = \theta^i(\Pi_0),\ i = 1, \dots, p-1$, and the prime ideals of $M$ over $p$ are noted $\mathfrak{p}$ or $\mathfrak{p}_j,\ j = 1 \dots, \nu$ where $\nu + 1$ is the number of such ideals.

**Theorem 6.5.** *Let $d$ be the order of $v\mu^{-1}$ mod $p$. There are $\frac{p-1}{d} + 1$ prime ideals in the singular primary $\mathbb{Q}$-field $M$ lying over $p$. Their prime decomposition and ramification is:*

1. $e(\mathfrak{p}_0/p\mathbb{Z}) = 1$.
2. $e(\mathfrak{p}_j/p\mathbb{Z}) = d$ *for all* $j = 1, \dots, \frac{p-1}{d}$ *with* $d > 1$.

*Proof.*

1. preparation of the proof
   (a) The inertial degrees verifies $f(\pi/p\mathbb{Z}) = 1$ and $f(\Pi/\pi) = 1$ and so $f(\Pi/p\mathbb{Z}) = 1$. Therefore, from multiplicativity of degrees in extensions, it follows that $f(\mathfrak{p}/p\mathbb{Z}) = f(\Pi/\mathfrak{p}) = 1$ where $\Pi$ is lying over $\mathfrak{p}$.
   (b) $e(\pi/p\mathbb{Z}) = p-1$ and $e(\Pi/\pi) = 1$ and so $e(\Pi/p\mathbb{Z}) = p-1$.
   (c) Classically, we get

$$\sum_{j=0}^{\nu} e(\mathfrak{p}_j/p\mathbb{Z}) = p, \tag{18}$$

   where $\nu + 1$ is the number of prime ideals of $M$ lying over $p$ and where $e(\mathfrak{p}_j/p\mathbb{Z})$ are ramification indices dividing $p-1$ because, from multiplicativity of degrees in extensions, $e(\mathfrak{p}_j/p\mathbb{Z}) \times e(\Pi/\mathfrak{p}_j) = p-1$.

2. Proof

   (a) The extension $S/M$ is Galois of degree $p-1$, therefore the number of prime ideals $\Pi$ lying over one $\mathfrak{p}$ is $\frac{p-1}{e(\Pi/\mathfrak{p})} = e(\mathfrak{p}/p\mathbb{Z})$.

   (b) Let $c(\Pi)$ be the orbit of $\Pi$ under the action of the group $< \sigma_\mu >$ of cardinal $p-1$ seen in lemma 6.4. If $\Pi = \pi_0$ then the orbit $C_\Pi$ is of length 1. If $\Pi \neq \pi_0$ then the orbit $C_\Pi$ is of length $d$. If $C_\Pi$ has one ideal lying over $\mathfrak{p}$ then it has all its $d$ ideals lying over $\mathfrak{p}$ because $\sigma_\mu(\mathfrak{p}) = \mathfrak{p}$. This can be extended to all $\Pi'$ lying over $\mathfrak{p}$ with $C_{\Pi'} \neq C_\Pi$ and it follows that when $\Pi \neq \pi_0$ then $d \mid e(\mathfrak{p}/p\mathbb{Z})$, number of ideals of $S$ lying over $\mathfrak{p}$. There is one $\mathfrak{p}$ with $e(\mathfrak{p}/p\mathbb{Z}) = 1$ because $C_{\pi_0}$ is the only orbit with one element.

   (c) The extension $S/M$ is cyclic of degree $p-1$. There exists one field $N$ with $M \subset N \subset S$ with degree $[N : M] = \frac{p-1}{d}$. If there were at least two different prime ideals $\mathfrak{p}'_1$ and $\mathfrak{p}'_2$ of $N$ lying over $\mathfrak{p}$, it should follow that $\mathfrak{p}'_2 = \sigma_\mu^{jd}(\mathfrak{p}'_1)$ for some $j$, $1 \leq j \leq d-1$ because the Galois group of $S/M$ is $< \sigma_\mu >$ and the Galois group of $N/M$ is $< \sigma_\mu^d >$. But, if a prime ideal $\pi_k$ of $S$ lies over $\mathfrak{p}'_1$ then $\sigma_\mu^d(\pi_k)$ should lie over $\mathfrak{p}'_2$. From lemma 6.4, $\sigma_\mu^d(\pi_k) = \pi_k$ should imply that $\mathfrak{p}'_2 = \mathfrak{p}'_1$, contradiction. Therefore the only possibility is that $\mathfrak{p}$ is fully ramified in $N/M$ and thus $\mathfrak{p}O_N = \mathfrak{p}'^{(p-1)/d}$. Therefore $e(\mathfrak{p}'/\mathfrak{p}) = \frac{p-1}{d}$ and so $e(\mathfrak{p}'/p\mathbb{Z}) = e(\mathfrak{p}/p\mathbb{Z}) \times \frac{p-1}{d} \mid p-1$ and thus $e(\mathfrak{p}/p\mathbb{Z}) \mid d$. From previous result it follows that $e(\mathfrak{p}/p\mathbb{Z}) = d$. Then $d > 1$ because $\mu - v \not\equiv 0 \mod p$ from Stickelberger theorem. There are $\frac{p-1}{d} + 1$ prime ideals $\mathfrak{p}_i$ because, from relation (18) $p = 1 + \sum_{i=1}^{\nu} e(\mathfrak{p}_i/p\mathbb{Z}) = 1 + \nu \times d$.

$\square$

**Example:** let us consider the case of prime numbers $p$ with $\frac{p-1}{2}$ prime.

1. Singular primary negative $\mathbb{Q}$-fields

   Here $\mu^{(p-1)/2} \equiv -1 \mod p$ and $d \in \{2, \frac{p-1}{2}, p-1\}$. Straightforwardly $d = 2$ is not possible: $\mu^2 \equiv v^2 \mod p$, then $\mu + v \equiv 0 \mod p$ because $\mu \not\equiv v \mod p$, then $\mu^{(p-1)/2} + v^{(p-1)/2} \equiv 0 \mod p$, contradiction because $\mu^{(p-1)/2} = v^{(p-1)/2} = -1$. $d = p-1$ is not possible because $\mu^{(p-1)/2} - v^{(p-1)/2} \equiv 0 \mod p$. Therefore $d = \frac{p-1}{2}$, so the ramification of $p$ in the singular $\mathbb{Q}$-field $M$ is $e(\mathfrak{p}_0/p\mathbb{Z}) = 1$ and $e(\mathfrak{p}_1/p\mathbb{Z}) = e(\mathfrak{p}_2/p\mathbb{Z}) = \frac{p-1}{2}$.

2. Singular primary positive $\mathbb{Q}$-extensions and primary unit $\mathbb{Q}$-fields

   Here $\mu^{(p-1)/2} \equiv 1 \mod p$ and $d \in \{2, \frac{p-1}{2}, p-1\}$. $d = 2$ is not possible : $\mu^2 - v^2 \equiv 0 \mod p$ then $\mu + v \equiv 0 \mod p$ so $\mu \equiv v^{(p+1)/2} \mod p$, so $B_{p-(p+1)/2} = B_{(p+1)/2} \equiv 0 \mod p$ where $B_{(p+1)/2}$ is a Bernoulli Number, contradiction because $B_{(p+1)/2} \not\equiv 0 \mod p$. $d = \frac{p-1}{2}$ is not possible because $\mu^{(p-1)/2} \equiv 1 \mod p$ and

$v^{(p-1)/2} \equiv -1 \mod p$. Therefore $d = p-1$, so the ramification of $p$ in the singular $\mathbb{Q}$-field $M$ is $e(\mathfrak{p}_0/p\mathbb{Z}) = 1$ and $e(\mathfrak{p}_1/p\mathbb{Z}) = p-1$.

**Acknowledgments:** I thank Professor Preda Mihailescu for helpful frequent e-mail dialogues and error detections in some intermediate versions of this paper.

# References

[1] D. Hilbert, *The Theory of Algebraic Number Fields, Zahlbericht*, Springer, 1998.

[2] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1982.

[3] R.A. Mollin, *Algebraic Number Theory*, Chapman and Hall/CRC, 1999.

[4] W. Narkiewicz, *Elementary and Analytic Theory of Numbers*, Springer-verlag, 1990.

[5] R. Quême, *On $\pi$-adic expansion of singular integers of the $p$-cyclotomic field*, arXiv.org, preprint math.NT/0610968

`\protect\vrule width0pt\protect\href{http://arxiv.org/PS_cache/math/pdf/0610/0610968.p`

[6] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[7] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2001.

[8] L.C. Washington, *Introduction to cyclotomic fields, second edition*, Springer, 1997.

Roland Quême
13 avenue du château d'eau
31490 Brax
France
mailto: roland.queme@wanadoo.fr
home page: http://roland.queme.free.fr/
***********************************
MSC Classification : 11R18; 11R29; 11R32
***********************************